Cloud Vendor Benchmark 2014

A Comparison of Software Vendors and Service Providers

Cloud Vendor Report

Executive Summary of the
Cloud Vendor Benchmark 2014 for

Trend Micro Incorporated

Cloud Leader 2014

Authors:

Oliver Schonschek & Heiko Henkes

Preface

While cloud computing adoption rates in Germany are on the rise, risks of data misuse and data losses are also increasing. Cloud users and providers are aware of these threats and are searching for secure solutions that enable them to leverage cloud computing benefits for their businesses and to ensure compliance with strict regulations, for instance regarding the privacy of data.

Many cloud consumers and providers are still challenged to take appropriate data encryption measures. Encryption of data transfers to a cloud service is quite common, but is not sufficient, since sensitive information is not encrypted once it has been transferred into to the cloud. And even if the respective cloud provider ensures the encryption of stored data, this is not necessarily enough to comply with German privacy regulations.

The cloud user, as the principal, remains responsible for protecting his data and must perform respective audits to ensure that the cloud provider has taken appropriate security measures. Privacy specialists urgently recommend that cloud users take cloud encryption into their own hands and encrypt their data, prior to transferring them into a cloud and independent of the respective cloud provider.

Trend Micro has realized this challenge early and provides a comprehensive cloud security portfolio for user organizations of all sizes and also for cloud service providers. A key component of the portfolio is the Trend Micro SecureCloud encryption solution, which can be purchased as a hosted service or installed and operated by the cloud users themselves. It ensures provider-independent cloud encryption and key management to enable cloud users to take care of cloud encryption themselves.

Cloud service providers, too, can benefit from Trend Micro SecureCloud: The solution is an important complement to be added to their own cloud portfolio to help their customers to ensure compliance with privacy regulations, certainly a unique selling proposition, since cloud users are increasingly aware of and addressing the cloud security issue.

Trend Micro received excellent ratings for the overall cloud security solutions portfolio and other criteria that were relevant for this Cloud Vendor Benchmark 2014, including the ease of use of the solution, professional support, support for multiple cloud environments and a high-class partner landscape, such as for Trend Micro SecureCloud, which helps both cloud users and service providers to ensure the required cloud encryption, while clearly reducing complexity and related efforts. Based on these benefits, Trend Micro was able to achieve top leadership positions in both cloud security categories (cloud security full stack and cloud security encryption) of this Cloud Vendor Benchmark 2014.

Oliver Schonschek

Munich, June 10, 2014

Oliver Schonschek
Research Follow

Deceptive Clouds Are Not an Obstacle

Although cloud computing is a business driver and represents the successful business models of modern times, these clouds are increasingly scrutinized; the larger the company, the stronger are related concerns, when it comes to sourcing or architecture blueprint decisions, due to increased regulation. There is no end to reports on hackers and US cyber sheriffs.

Information based on the “Snowden papers” and disclosed to the public, including users and vendors of cloud technologies and services, have caused significant suspicion and distrust when it comes to storing data “in the Internet”, i.e., “in the cloud”.

In Germany, the fear of the NSA's access to data is mixed with the fear of “normal” cyber-attacks, theft of user data, manipulation of databases etc. – and understandably so; but nevertheless, this prevents people to have a clear view of the reality and also potential solutions.

As a rule, systems that are used to store and process data must be protected against unauthorized access, manipulation and loss. A look at the afore-mentioned “normal” cyber-attacks reveals that such attacks are successful because basic security requirements were ignored or mechanisms for risk detection and prevention were not enforced consistently. Consistency is key here, since today's attackers just have a condescending smile for the former “hard shell, soft center” philosophy. The magic word is defense in depth, which means that all systems and all kinds of system access, be it physical or logical, are secured on all levels. It is not sufficient any more to secure the physical server where the virtualized systems reside. Rather, all connections to and from cloud data centers must provide strong protection, since this is one of the NSA's main attack vectors, as large American Internet companies have painfully experienced.

Cloud Security Technologies

Basic cloud security criteria include a decentralized structure and a multitude of connections and access points required to ensure the fast and flexible usage of data and applications. Cloud security implies the complete high-level protection of infrastructures, connections, devices, applications and data, also because enterprise networks are no longer closed systems with only few, easy-to-control access points. Today, a company is a value-added network connecting thousands of partners, suppliers and users through core applications and processes. With integrated cloud strategies that also link traditional enterprise systems such as ERP, databases, HR etc. with modern cloud applications and mobile apps, there is no hard shell any more to protect the heart of the enterprise. A flexible and scalable in-depth security strategy is required to provide comprehensive protection of all cloud components.

This chapter examines and evaluates the offerings and competitive strength of security vendors in the German market who support cloud data center operators to help them secure and monitor their cloud infrastructures and cloud services. The analysis is mostly based on the breadth and depth of offerings required to ensure the integrated protection and proactive security management of users' cloud environments.

Core cloud security segments include the following:

- Business continuity & disaster recovery;
- Data center operations & network security;
- Incident response;
- Application security;
- Identity & access management;
- Virtualization security.

Evaluation of Individual Providers

Within the cloud security technologies category, ten out of 22 relevant providers were positioned in the leader quadrant. F-Secure is positioned as Rising Star. Within its cloud vendor benchmark, Experton Group has examined whether security products have been modified to address the complex requirements of cloud environments and the rapidly evolving threats landscape. Key requirements include better protection of virtual environments against external and cloud-internal attacks and also against malware and Trojans, which have become even more dangerous, including advanced persistent threat (APT) attacks.

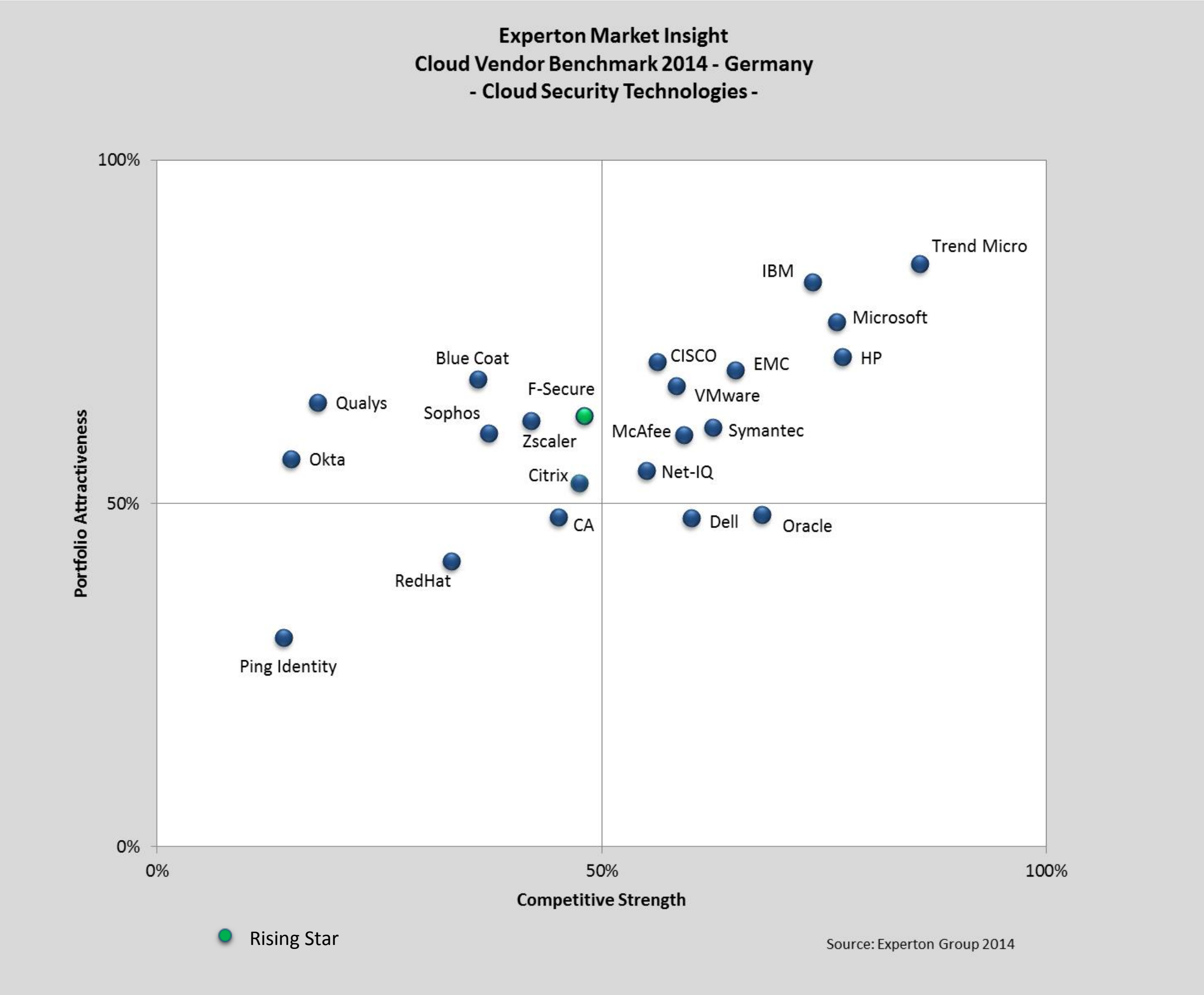


Figure 1: Cloud security technology vendors

Trend Micro Evaluation

Trend Micro was able to maintain its top leadership position from last year's cloud vendor benchmark, due to the consistent alignment of its overall strategy towards cloud security. With Deep Security, Trend Micro's solution to help customers protect operating systems, applications and data on physical, virtual and cloud-based servers, the vendor meets the key requirements, as specified by the Experton Group analysts, to provide in-depth protection of virtual and cloud environments against external and cloud-internal attacks. “Deep Security for Web Apps” provides additional protection for web applications and online shops within data centers or in the cloud. The solution detects vulnerabilities without annoying false alarms and provides protection before these security holes can be exploited accordingly, avoiding emergency patching, problems with application updates and costly system failures. “Deep Security for vCloud Hybrid Service“ allows customers to easily enhance and extend the security of existing installations to also include cloud workloads. Interoperability with “VMware vCloud Director“ and other VMware technologies enables administrators to automatically detect virtual machines and apply respective context-based policies to ensure consistent security levels across the data center and the public cloud. This strong focus on cloud security is also reflected in the successful common criteria certification of Deep Discovery Inspector, according to BSI (German Federal Office for Information Security). The Broadweb acquisition has further increased Trend Micro's capabilities for malware and in particular APT detection. For Experton Group, Trend Micro's increased integration with third-party cloud security solutions (e.g. VMware NSX) further substantiates the vendor's leadership position.

Analyst Statement

“As of today, Trend Micro provides the most extensive portfolio for flexible and scalable in-depth security strategies to help customers ensure the comprehensive protection of all cloud components.”

Cloud security encryption

Encryption is the “silver bullet” for protecting sensitive data. Strong encryption of cloud access points and cloud storage is important, but is not enough; cloud users must also encrypt their cloud environments with state-of-the-art technology and independent of the respective cloud provider.

Various options are available for such provider-independent encryption:

1. Encryption solutions that provide an explicit cloud functionality, i.e., specific cloud interfaces and transfer data into the cloud after they have been encrypted;

2. Professional cloud storage and collaboration solutions that feature specific encryption functionality, since encryption is a critical requirement for cloud storage and cloud collaboration.
3. Cloud security solutions that feature provider-independent encryption for data in a cloud and are used in addition to cloud management solutions; and
4. Encryption solutions that encrypt sensitive data locally and leave data transfer into the cloud to a separate solution. Since these are no explicit cloud encryption solutions, they will not be analyzed within the benchmark.

For the purpose of this Cloud Vendor Benchmark, Experton Group has examined the solution variants 1 to 3 and has analyzed respective offerings for cloud data encryption. This included solutions that have been designed for business users and also help ensure compliance with respective privacy requirements.

Evaluation of Relevant Providers

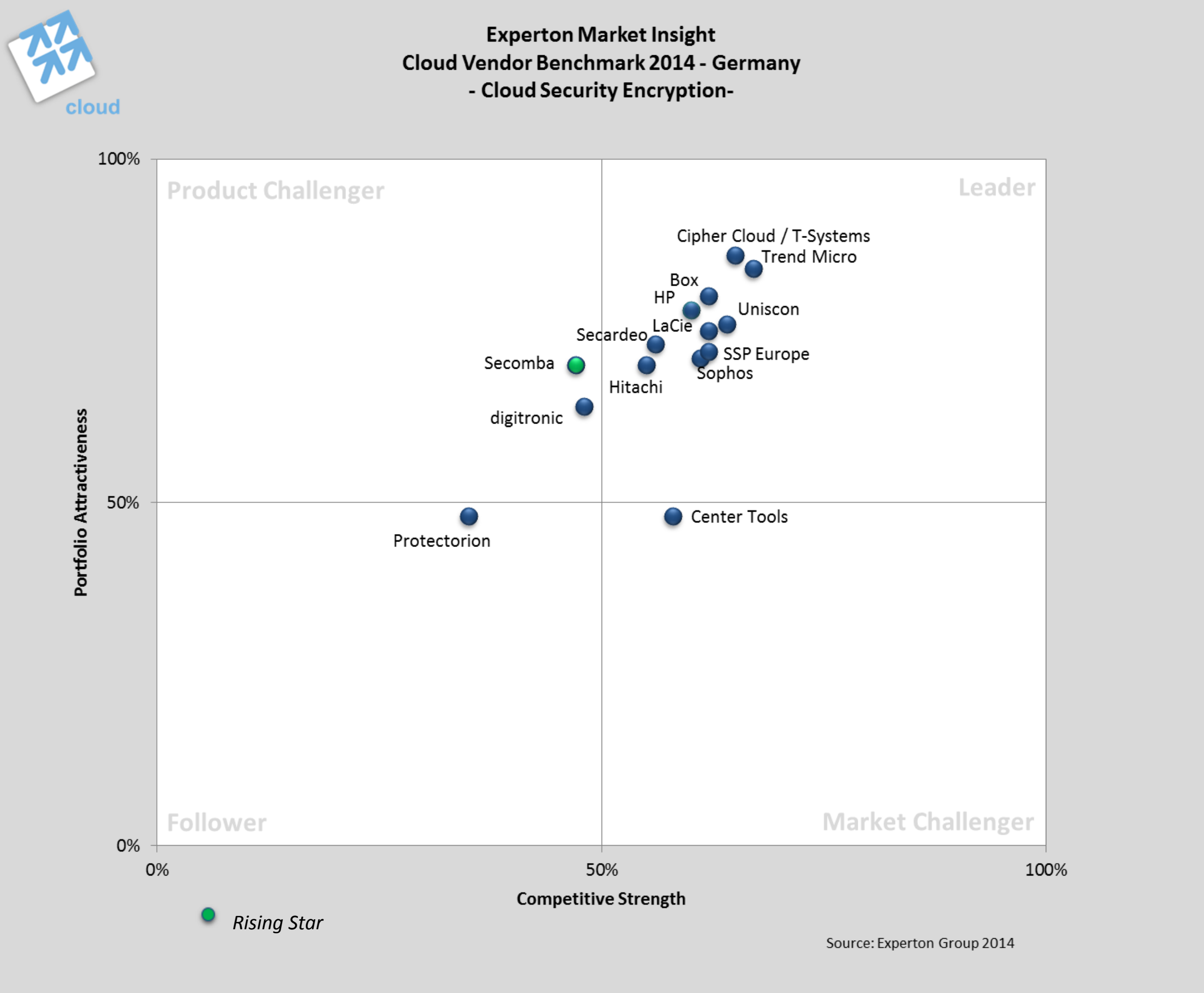
14 out of the multitude of available encryption solutions have met the analysis criteria, i.e., they address cloud data encryption and the high requirements of business users, while also accounting for privacy and compliance with respective regulations – with varying degrees of success. Ten vendors and their cloud encryption solutions were positioned in the leader quadrant: Trend Micro, Cipher Cloud, Box, Uniscon, HP, SSP Europe, La Cie, Sophos, Secardeo and Hitachi HDS. Secomba with its Boxcryptor solution was identified as Rising Star and has the potential to be positioned in the leader quadrant mid-term.

Trend Micro Evaluation

Trend Micro (with Trend Micro SecureCloud) and CipherCloud (with CipherCloud for any App) address the end-to-end encryption challenge with a centralized solution approach. Cloud encryption has no focus on individual cloud services, but can be used by user organizations for their individual cloud infrastructure. Both solutions provide provider-independent cloud encryption, which is decisive for ensuring the privacy of data and which means that the encryption key remains with the user organization. Trend Micro SecureCloud and CipherCloud for any

Analyst Statement

> *"Trend Micro and CipherCloud provide comprehensive support to help users achieve standardized end-to-end encryption of their cloud data, with encryption keys remaining in the hands of the respective user company."*



Source: Experton Group 2014

Figure 2: Cloud Security Encryption

App address the enterprise user segment; Trend Micro SecureCloud is also available for cloud service providers as an important extension to ensure data security and privacy.

About Trend Micro

As the global leader in cloud security, Trend Micro secures the digital information exchange of companies and end users. Trend Micro is a server security pioneer with more than 25 years of experience. The Trend Micro security solutions prevent threats where they occur – in the Internet – and provide comprehensive protection of data in physical, virtual and cloud environments. The company is headquartered in Tokyo.

About Experton Group

Experton Group is a leading IT research, advisory and consulting house. The company has 30 experienced analysts in Europe who support mid-sized and large organizations with their IT strategic planning and implementation. In Germany, Experton Group has offices in Munich, Frankfurt and Kassel.

More information on our research can be found under: www.experton-group.de

Contact

Experton Group AG
Carl-Zeiss-Ring 4
D-85737 Ismaning
Tel. +49 89 923331-0
Fax +49 89 923331-11

Authors

Heiko Henkes,
Manager Advisor & Project Manager
Heiko.henkes@experton-group.com

Oliver Schonschek
Research Fellow
oliver.schonschek@experton-group.com